

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of) **MAIL STOP**
Carine Boursier et al.) Group Art Unit: 2617
Application No.: 10/583,120) Examiner: Obayanju, Omoniyi
Filed: June 16, 2006) Confirmation No.: 1809
For: METHOD OF SECURING A)
MOBILE TELEPHONE IDENTIFIER)
AND CORRESPONDING MOBILE)
TELEPHONE)

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants request review of the final rejection of claims 2, 4-7 and 9-20 set forth in the Office Action dated February 16, 2011. This Request is being filed with a Notice of Appeal. No amendments are being filed with the Request.

In the Advisory Action dated July 7, 2011, under the heading "AMENDMENTS", box 3 is checked, indicating that the Amendment filed June 16, 2011 will not be entered. However, box 7 is also checked, and states that the Amendment will be entered. In a telephone conversation with Examiner Obayanju on July 12, 2011, he confirmed that the Amendment will be entered, and that it overcomes the rejection under 35 USC 112, paragraph one. Accordingly, the only issue to be reviewed is the rejections under 35 USC 103.

Background

The Review Panel is referred to the Remarks section of the Amendment filed June 16, 2011, at pages 9-10, for a brief discussion of the problem being addressed by the claimed invention, and the approach taken by the inventors to solve that problem.

Argument

Claims 18, 19 and 20 are the currently pending independent claims. Claim 18 recites, among other elements, a memory containing program instructions that control a handset to perform the following operations:

authenticate, by the secure electronic module, the storage support module;

establish, in the event the secure electronic module determines that the storage support module is authentic, a secure communication channel between the storage support module and the secure electronic module;

transmit, via the secure communication channel, the IMEI from the storage support module to the secure electronic module ...

Method claim 19 and apparatus claim 20 recite the same or similar features.

For purposes of this review, the Panel is requested to focus upon two claimed concepts, namely (1) the authentication of the storage support module by the secure electronic module, and (2) in the event that the storage support module is authenticated, establishing a secure communications channel between the storage support module and the secure electronic module. For the reasons presented hereinafter, the final Office Action has not established that either of these claimed concepts are disclosed in the references. Consequently, the issues are not in a posture that is ripe for consideration by the Board of Patent Appeals and Interferences.

In connection with the authentication of the storage support module by the secure electronic module, the Office Action asserts that this feature is disclosed in the Simmons Patent Application Publication (US 2004/0043792), at page 3, paragraph 0030. This paragraph merely discloses that the mobile station (MS) 10 has a SIM 20 and a mobile equipment identity (IMEI) unit 15. Thus, it discloses structure corresponding to a secure electronic module and a storage support module, respectively. However, it does not disclose that the SIM 20 operates to **authenticate** the IMEI unit. Consequently, the only portion of the reference that is cited to support the rejection does not disclose the claimed feature for which it is being relied upon.

It is to be noted that, beginning at paragraph 0039, Simmons discloses that the SIM 20 authenticates the MS 10. However, authentication of the mobile station

itself is not the same as, nor suggestive of, authentication of the IMEI unit 15. To understand this distinction, it is useful to review the background portion of the reference.

Beginning at paragraph 0010, Simmons describes that a SIM card can store a prepaid amount of money to permit network usage for a certain amount of time. However, if a mobile terminal is not equipped to decrement the stored amount during network usage, unauthorized use of the network, beyond the prepaid time, could occur. As stated at the end of paragraph 0011, “there is nothing specified to date that allows for the SIM to recognize and allow or disallow registration with certain terminal devices.” Simmons is directed to the “need for an apparatus and method where only approved pre-paid MS’s are used in conjunction with their pre-paid SIM cards” (end of paragraph 0013). To this end, therefore, Simmons discloses that “a SIM containing data on prepaid time may challenge the terminal device MS prior to reporting its IMEI value to the MS, so that the terminal device can make calls only if it is capable of decrementing the stored value” (paragraph 0017).

Returning to paragraph 0039, after stating that the SIM card 20 authenticates the mobile station 10, Simmons goes on to explain that this is done “to externally *verify that the terminal device is compatible with pre-paid operation* by generating a random number and sending it to the ME 10...” (emphasis added)¹. To this end, the reference also discloses that the manufacturer of the ME “will only put the code for processing the random value and the key in ME’s that are equipped with decrementing engines...” (paragraph 0047).

Thus it can be seen that, in Simmons, the SIM only authenticates the mobile terminal itself, to determine whether it is capable of decrementing prepaid minutes. There is no disclosure that the SIM authenticates a storage support module, e.g. the IMEI unit 15. There is no need to do so in the context of Simmons, because it is directed to a different problem from that addressed by the claimed invention.

The Advisory Action refers to paragraph 0041 in connection with this claimed feature. This cited paragraph states that the key used to authenticate the ME can be based upon the ME’s IMEI. However, the fact that the key used to perform the authentication is derived from the IMEI in no way suggests that the SIM actually

¹ The term “ME” is used interchangeably with the term “MS” in the patent to denote the mobile station.

authenticates the module in which that IMEI is stored. Simmons is only concerned with pre-paid features and not the integrity of the IMEI. As such, there is no reason to authenticate the IMEI unit 15.

For at least these reasons, the final Office Action fails to establish that Simmons discloses this first claimed feature.

Turning now to the second feature, the final Office Action asserts that the establishment of a secure communications channel between a storage support module and a secure electronic module is disclosed in Simmons at paragraphs 0042 and 0049. Paragraph 0042 pertains to the authentication of the mobile station by the SIM, discussed above. It has nothing to do with secure communications between the SIM and the IMEI unit 15.

Paragraph 0049 pertains to an option by which the SIM can be locked to a single ME, rather than being used with multiple MEs. The panel is referred to the first full paragraph on page 12 of the June 16 Amendment for a discussion of this portion of Simmons. As noted therein, the cited paragraph does not disclose a secure communications channel between the SIM and the IMEI unit.

The final Office Action also relies upon the Portalier et al patent (GB 2355892) as allegedly disclosing a secure communications channel between a storage support module and a secure electronic module. Particular reference is made to page 3, lines 21-26 and the phrase “coupling, ... by means of an encryption algorithm, between the IMSO subscriber identity code of the SIM card and the IMEI identity code of the mobile telephone...” However, this “coupling” has nothing to do with communications between the SIM card and the memory storing the IMEI. Rather, it pertains to binding a particular SIM to a given mobile telephone’s IMEI, to discourage theft. In essence, it is analogous to what is disclosed in paragraph 0049 of Simmons.

The “encrypted” nature of the coupling also has nothing to do with secure communications between the SIM and the IMEI memory. To perform the binding, or coupling, Portalier discloses that a code called “SecretE” is produced as a function of the identity code IMSO of the SIM. In one embodiment, the code “SecretE is produced by an encryption that is parameterised, for example, by the IMEI identification code of the mobile telephone ... to resist unlocking moves” (page 6,

lines 8-15). In other words, the IMEI is used to provide parameter values for the algorithm that encrypts the IMSO to produce the code SecretE. Portalier does not disclose that, as part of this process, secure communications are carried out between the SIM card and the memory module storing the IMEI.

Thus, the final Office Action has not provided any interpretation of Simmons or Portalier demonstrating that either of these references discloses the establishment of a secure communications channel between a storage support module, e.g. memory storing an IMEI, and a secure electronic module, such as a SIM card. Moreover, there is no showing that such establishment occurs on the condition that the storage support module is first authenticated by the SIM, as recited in the claim. The cited passages of the references have nothing to do with communications between these two components in a telephone handset.

Although the foregoing discussion is directed to claim 18, the same arguments apply to independent claims 19 and 20.

Conclusion

In summary, the final Office Action does not demonstrate that the cited references disclose, or can be interpreted to disclose, all of the elements of the claims. In particular, there is no support in the references for the assertion that they disclose (1) authentication of a storage support module by a secure electronic module, or (2) establishing a secure communications channel between a storage support module and a secure electronic module.

The grounds of rejection are factually defective, since they fail to establish a *prima facie* case of obviousness. As such, the issues are not ripe for consideration by the Board of Appeals and Interferences. Further action in the form of re-opening prosecution based upon new prior art, or a Notice of Allowance, is submitted to be in order, and is respectfully requested.

Respectfully submitted,
BUCHANAN INGERSOLL & ROONEY PC

Date: July 18, 2011

By: /James A. LaBarre/

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

James A. LaBarre
Registration No. 28632